Whistler Design Preview
April 20 & 21

Enhancements to Active Directory in Whistler

Stuart Kwan
Server Product Group
Microsoft Corporation

Whistler Goals

- General engineering improvements
  - Performance
  - General code improvement
  - Bug fixes
- Lower barriers to deployment
  - Scalability
  - Management and monitoring
- Continue to enhance platform

Technologies Covered

- Core DS
- Replication
- DNS & naming
- ADSI & LDAP
- DS admin UI

Simplify Deployment (1/11)
Core DS

- Scalability issue: must replicate GC into remote site for native mode logon

Simplify Deployment (2/11)

Core DS

- Feature: No-GC logon
  - DC caches user's group membership
    - Only for users that logon to that DC
    - Refresh cache on periodic basis
    - Cache is always used when populated
  - Optimal for site with single DC

Simplify Deployment (3/11)

Core DS

- Scalability issue: difficult to create replicas of a large domain
  - Large amount of bandwidth used to replicate large domain to remote site
    - Difficult to bootstrap branch office
  - Extended length of time required to create replica of large domain, even over LAN
    - Difficult to add more DCs/more

Simplify Deployment (4/11)

Core DS

- Feature: create replica from media
  - New option in DCPROMO
    - Populate DS from files instead of net
    - Use backup & restore to transport files
    - Works for GCs
    - Network connectivity still required

Simplify Deployment (5/11)

Replication

- Scalability issue: group membership replicates as single unit
  - Multi-master - can lose updates
  - Sub-optimal bandwidth usage

Simplify Deployment (6/11)

Replication

- **Feature: replicate membership deltas instead of entire membership**
  - **Store metadata for each value**
  - **Only for *linked-value* multi-valued attributes**
  - **Also eliminates 5000 member limit**
  - **Only works between Whistler DCs**

Simplify Deployment (7/11)
Replication

- Scalability issue: GC performs full sync if attributes added to GC partial attribute set

Simplify Deployment (8/11)

Replication

- Feature: no GC full sync when adding attributes to GC partial attribute set
  - Replicate added attributes only
  - Requires GC replication partners are upgraded to Whistler
    - System does best-effort to select uplevel partners

Simplify Deployment (9/11)
Replication

- Scalability issue: for large # of sites KCC is impractical
  - Admin must hand configure replication connections
  - Admin may be required to manually account for failed networks/servers

Simplify Deployment (10/11)

Replication

- Feature: Inter-site repl topology tool
  - Creates LDIF file of inter-site connections
  - Admin runs periodically, imports connections into DS
  - Algorithms to be incorporated into KCC post-Whistler

Simplify Deployment (11/11)

DNS and Naming

- Domain controller rename
- DNS server and client
  - BIND parity
    - Conditional forwarding
    - Stub zones
    - Minimal support for DNSSEC
  - WMI provider to programmatically configure DNS server
  - Control client settings via group policy

Management & Monitoring

Admin Tools

- Users and Computers snapin
  - Drag and drop
  - Multi-select-and-edit user objects
  - Saved queries
- ACL editor
  - Reset permissions to schema default
  - Show effective permissions for user/group
  - Show parent of inherited

Management & Monitoring

Admin Tools

- Revised Object Picker
  - Search rather than browse
  - Improved scalability

Management & Monitoring

WMI providers

- Replication monitoring via WMI
  - Replication status on DC-by-DC basis
  - Plugs into HealthMon framework
  - Minimal “thumbs up/thumbs down” status
- Trust monitoring

Enhance Platform (1/3)
Core DS

- **Issue: impractical to store rapidly-changing data in the DS**
  - **Replicates to all DCs in a domain or does not replicate at all**
  - **Many replicas == high latency**
  - **Data may be replicating to places it is not needed**

Enhance Platform (2/3)
Core DS

- **Feature: Non-domain naming context**
  - **Instantiate NDNC on any DC in forest**
  - **Place replica copies on other DCs in forest as desired, to scope replication**
  - **Observes schedule like other NCs**
  - **Can contain any hierarchy of objects except security principals**

Enhance Platform (3/3)
LDAP & ADSI

- Virtual List Views (VLV)
- Correct Aux class support (X.501)
  - Apply Aux class to object instance
  - Necessary for interoperability
- Dynamic entries (RFC 2589)
  - Object assigned Time To Live (TTL)
  - Object automatically deleted after TTL
- Unified path for ADSI & WMI

Behavior Versioning (1/2)

Necessary Evil

- Active Directory Behavior Versioning
  - Generalized “Native Mode”
  - Required in order to introduce non-backward-compatible features
  - Admin can advance version number when all DCs in scope are upgraded
    - Domain behavior version
    - Forest behavior version
  - Version numbers can only increase

Behavior Versioning (2/2)

- Requires *Forest version == Whistler*
  - Group membership replication
- Requires *Domain version == Whistler*
  - Active Directory integrated stub zones

Not in Whistler

- Domain rename
- Move domain between forests
- Schema delete
- Schema per domain
- Multiple domains per DC
- Read-only naming contexts
- Inter-domain policy/ACL propagation
- Intra-domain SMTP replication
- Per-OU password policy


Where do you want to go today?®
Microsoft